PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-341324
(43)Date of publication of application : 08.12.2000

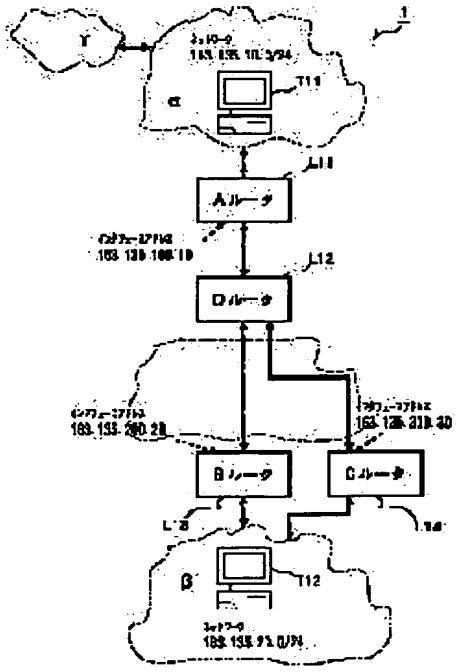
(51)Int.Cl. H04L 12/56
H04L 9/08
H04L 12/46
H04L 12/28
H04L 12/22
H04L 29/14

(21)Application number : 11-146948
(22)Date of filing : 26.05.1999

(71)Applicant : NTT DATA CORP
(72)Inventor : KUSAKA TAKAYOSHI
MATSUDA YOSHIYUKI
BABA TATSUYA

(54) CIPHER COMMUNICATION METHOD AND SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To realize a cipher communication system that can continues cipher communication even when a decoder is changed due to a path change on the occurrence of a path fault during the cipher communication.
SOLUTION: Layout information relating to the layout of other routers L12 to L14 capable of cipher communication is included in path forming information of a router L11 that receives are transmits the path information such as a routing protocol. In the case that any router such as the router L13 on an optimum path during the cipher communication is disabled of communication, a new optimum path is formed again and continues the cipher communication with the other router L14 in existence on the optimum path formed again by using a key decided mutually.



LEGAL STATUS
[Date of request for examination] 09.12.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－341324
（P2000－341324A）
(43)公開日　平成12年12月８日(2000.12.8)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　11/20	１０２Ｄ	５Ｊ１０４
9/08		9/00	６０１Ｚ	５Ｋ０３０
12/46		11/00	３１０Ｃ	５Ｋ０３３
12/28		11/26		５Ｋ０３５
12/22		13/00	３１１	９Ａ００１

審査請求　未請求　請求項の数10　ＯＬ　（全 9 頁）　最終頁に続く

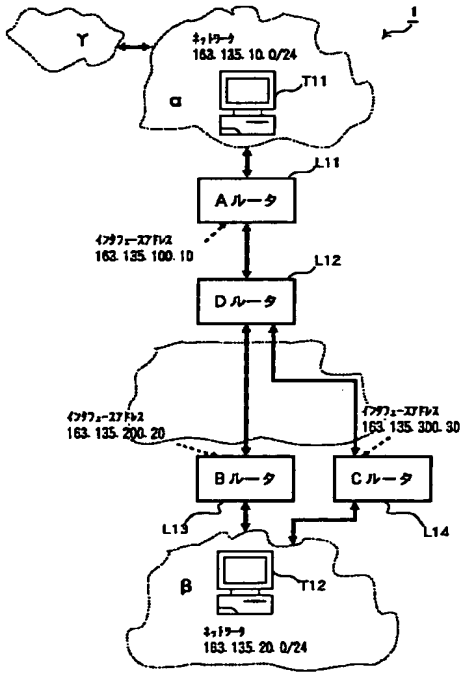
(21)出願番号　特願平11－146948
(22)出願日　平成11年５月26日(1999.5.26)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　日下　貴義
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　松田　栄之
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(74)代理人　100099324
弁理士　鈴木　正剛

最終頁に続く

(54)【発明の名称】　暗号通信方法及びシステム

(57)【要約】
【課題】　暗号通信中に経路障害が発生し、経路変更に伴って復号化を行う装置が変わった場合にも暗号通信を継続できる暗号通信システムを実現する。
【解決手段】　ルーティングプロトコルのような経路形成情報の受け渡しを行うルータＬ１１の経路形成情報に、暗号通信可能な他のルータＬ１２～Ｌ１４の配置に関する配置情報を含める。暗号通信中の最適経路上のいずれかのルータ、例えばルータＬ１３が通信不能になったときは、新たな最適経路を再形成するとともに、再形成された最適経路に存する他のルータＬ１４との間で相互に取り決めた鍵を用いて暗号通信を継続する。



1

【特許請求の範囲】

【請求項１】　高可用通信と暗号通信とを同時に実現することができるネットワークを介して行う暗号通信方法であって、

前記ネットワーク上で暗号通信可能な通信中継装置の配置に関する配置情報を含む所定の経路形成情報を複数の通信中継装置間で互いに交換しあうことによりネットワーク上における最適経路を形成し、この最適経路に存在する通信中継装置間で通信データの暗号通信を行うとともに、前記ネットワーク上における通信中継装置の構成が変更された場合に前記経路形成情報を更新して新たな最適経路を再形成し、再形成された最適経路に存する暗号通信可能な通信中継装置間で相互に取り決めた鍵を用いて前記暗号通信を継続することを特徴とする、

暗号通信方法。

【請求項２】　各通信中継装置は、ある通信装置又はネットワークへ向かう暗号化された通信データの復号化ができる場合にその通信装置又はネットワークの識別情報を記録しておき、他の通信中継装置から前記経路形成情報を受け取ったときに暗号通信先が前記識別情報と同じ識別情報を保持していた場合に、前記他の通信中継装置との間で前記鍵の取り決めを行うことを特徴とする、

請求項１記載の暗号通信方法。

【請求項３】　所定の経路形成情報を複数の通信中継装置間で互いに交換しあうことにより高可用通信と暗号通信とを同時に実現することができるネットワーク上における最適経路を形成し、この最適経路に存在する通信中継装置間で通信データの暗号通信を行う暗号通信システムであって、

各通信中継装置の経路形成情報は、前記ネットワーク上で暗号通信可能な通信中継装置の配置に関する配置情報を含むものであり、

前記複数の通信中継装置の少なくとも一つは、暗号通信中の最適経路上の通信中継装置の配置構成が変更になったことを検知したときに当該変更後の配置情報を他の通信中継装置に通知するように構成され、少なくとも他の一つは、前記通知をもとに自己の経路形成情報を更新して新たな最適経路を再形成するとともに再形成された最適経路に存する暗号通信可能な通信中継装置間で相互に取り決めた鍵を用いて前記暗号通信を継続するように構成されていることを特徴とする、

暗号通信システム。

【請求項４】　所定の経路形成情報をもとに高可用通信と暗号通信とを同時に実現することができるネットワーク上における最適経路を形成するとともにこの最適経路に存在する他の通信中継装置との間で暗号通信を行う通信中継装置であって、

前記経路形成情報は、暗号通信可能な通信中継装置の配置に関する配置情報を含むものであり、

暗号通信中に前記最適経路における他の通信中継装置の

2

配置構成が変更になった場合に自己の経路形成情報に含まれる前記配置情報の内容を更新する更新手段と、

更新後の経路形成情報をもとに新たな最適経路を形成する経路形成手段と、

新たに形成された最適経路上の暗号通信可能な他の通信中継装置を検出する検出手段とを備え、

当該検出した通信中継装置との間で取り決めた鍵を用いて暗号通信を継続することを特徴とする、

通信中継装置。

【請求項５】　前記経路形成情報が所定のルーティングプロトコルに基づいて他の通信中継装置との間で相互に受け渡しされる情報であって、暗号通信を行えるノードの配置に関する情報及びそのノードが暗号通信実施の対象とする通信経路の識別情報を含むものであり、前記識別情報に基づいて前記鍵を取り決めることを特徴とする、

請求項４記載の通信中継装置。

【請求項６】　前記識別情報をもつノードとの間で取り決めた鍵を予め保持している場合はその鍵を索出し、鍵を保持していない場合は当該ノードとの間で鍵生成を行うことで前記鍵を確保することを特徴とする、

請求項５記載の通信中継装置。

【請求項７】　前記更新手段は、暗号通信中に通信不能となった通信中継装置に関する配置情報を削除するように更新することを特徴とする、

請求項４記載の通信中継装置。

【請求項８】　前記更新手段は、暗号通信中に増設された通信中継装置に関する配置情報を追加するように更新することを特徴とする、

請求項４記載の通信中継装置。

【請求項９】　前記更新手段は、暗号通信中に移動された通信中継装置に関する配置情報を修正するように更新することを特徴とする、

請求項４記載の通信中継装置。

【請求項１０】　暗号通信可能な通信中継装置の配置に関する配置情報を含む所定の経路形成情報をもとに、高可用通信と暗号通信とを同時に実現することができるネットワークネットワーク上における最適経路を形成する機能と、

通信相手装置との間で暗号通信を行う機能と、

前記通信相手装置の構成が変更になった場合に自己の経路形成情報に含まれる前記配置情報の内容を更新し、更新後の経路形成情報をもとに新たな最適経路を形成するとともに、この新たな最適経路に存在する他の通信相手装置との間で取り決めた鍵を用いて暗号通信を継続する機能とをコンピュータ上に形成するためのプログラムコードが記録された、コンピュータ読みとり可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、高可用通信（障害時でも経路切替による自動継続が可能な通信、つまり耐障害性をもつ通信、以下同じ）と暗号通信（暗号技術を利用した機密通信、以下同じ）とが同時に実現できるネットワークにおいて、暗号通信中に通信中継装置の構成の変更が生じ、最適経路が変化した場合であっても暗号通信を安全に継続できるようにするための暗号通信技術に関する。

【０００２】

【従来の技術】ＩＰ（Internet Procotol）ネットワークを使用して行う暗号通信の形態は、従来より良く知られている。この種の暗号通信は、送信側の暗号化装置と受信側の復号化装置との間で生成した鍵（暗号鍵／復号鍵）を用いて行われる。この場合の通信の形態としては、エンド・ツー・エンドで暗号通信を行う形態と、通信経路上に通信データ、例えばパケットの暗号化及び復号化を行う通信装置（以下、「暗号装置」）を配置することによって暗号通信を行う形態とがある。

【０００３】ＩＰネットワークにおいて暗号通信に用いる鍵の生成、鍵交換、鍵設定の手順としては、例えばＩＫＥ（Internet Key Exchange：暗号鍵生成手順）方式等、様々な手法が存在する。送信側は、この生成された鍵（暗号鍵）を使用してＩＰパケットを暗号化し、受信側は、この鍵に対応した鍵（復号鍵）を用いてパケットを復号化する。

【０００４】ところで、ＩＰネットワークを使用して通信を行っている最中に最適経路に何らかの障害が発生した場合は、ＯＳＰＦ（Open ShortestPath First）等のルーティングプロトコルを使用したり、ルータ等の通信中継装置自身の持つバックアップ経路設定機能を使用したりして通信を回復させることができる。つまり、自動的に迂回経路を設定して通信を回復させることができる。以下、これらの通信回復方法の概要を説明する。

【０００５】（１）ルーティングプロトコルを使用した場合

図６に示すように、通信装置Ｔ１１と通信装置１２との間のＩＰネットワーク上のノードにルータＮ１１～Ｎ１５が接続されているとする。正常時の最適経路は、通信装置Ｔ１１→ルータＮ１１→ルータＮ１２→ルータＮ１３→ルータＮ１５→通信装置Ｔ１２、あるいはその逆であり、各ルータＮ１１～Ｎ１５は、互いに持っている経路形成情報、すなわち各ルータが直接どのルータと通信可能か等を表す情報を交換し合い、ネットワーク間の最適経路を形成している。

【０００６】この最適経路において、ルータＮ１３に障害が発生した場合は、以下のような手順で通信の回復を行う。まず、ルータＮ１３に隣設する正常なルータ、例えばルータＮ１２が、ルーティングプロトコルの機能により、ルータＮ１３に障害が発生したことを検知する。検知方法は、ルーティングプロトコルによって決められている。障害を検知したルータＮ１２は、「今までの経路が使用できなかったこと」や「リンクが無くなったこと」等の情報を、ルーティングプロトコルの機能により、隣接するルータＮ１１，Ｎ１４に通知する。これらの通知情報は、隣接するルータＮ１５にもリレーされ、これによりルーティングドメイン（ルーティング情報を受け渡すルータのグループ）のすべてのルータに通知される。このように新しく通知される情報により、各ルータＮ１１，Ｎ１２，Ｎ１４，Ｎ１５が持つ経路形成情報は更新され、障害経路の代わりになる迂回経路、すなわち、通信装置Ｔ１１→ルータＮ１１→ルータＮ１２→ルータＮ１４→ルータＮ１５→通信装置Ｔ１２の経路が再形成される。

【０００７】（２）バックアップ経路設定機能を使用した場合

図６に示した通信システムの中のあるルータ、例えばルータＮ１２にバックアップ経路設定機能があり、ルータＮ１２が中継経路に障害が発生したことを検知した場合（リンクの有無やポーリング（監視信号）、キープアライブ（回線がダウンしていないことを確かめるための信号）等による）、ルータＮ１２は、バックアップ経路設定機能に基づいて、予め設定しておいた代替経路（バックアップ経路）に切り替えて通信を保つ。

【０００８】

【発明が解決しようとしている課題】通常通信のみならず、暗号通信を行っている最中に最適経路に障害が発生した場合も、上記のルーティングプロトコルの機能やバックアップ経路設定機能を用いて迂回経路を形成することができる。しかしながら、暗号通信の場合は、ルーティングプロトコルの機能あるいはバックアップ経路への切替機能と暗号通信の機能とが別構成になっているため、既存の仕組みのままでは、暗号化されたＩＰパケット（暗号化データ）を復号化することができず、暗号通信を継続できない場合がある。このことを以下に説明する。

【０００９】ここでは、図７に示す構成、すなわち、ルータＮ１２に暗号装置Ｍ２１を介して通信装置Ｔ１１が接続され、ルータＮ１５に通信装置Ｔ２２が接続され、さらにルータＮ１２とルータＮ１５との間に、それぞれ暗号装置Ｍ２２，Ｍ２３が並列に接続されたＩＰネットワーク構成を想定する。

【００１０】各ルータＮ１２，Ｎ１５及び暗号装置Ｍ２１，Ｍ２２は、互いに持っている経路形成情報を交換しあい、ネットワーク間の最適経路を形成している。正常時における最適経路、つまり通常経路で収束した場合の経路は、通信装置Ｔ１１→暗号装置Ｍ２１→ルータＮ１２→暗号装置Ｍ２２→ルータＮ１５→通信装置Ｔ１２であり、暗号装置Ｍ２１は、通信装置Ｔ２２から送信されるパケットを、自装置と暗号装置Ｍ２２との間で用いられる鍵（例えば鍵Ａ）を用いて暗号化する。

5

【００１１】この状態で、暗号装置Ｍ２２で何らかの障害が発生し、ルーティングプロトコルの機能により経路変更が行われ、最適経路が通信装置Ｔ１１→暗号装置Ｍ２１→ルータＮ１２→暗号装置Ｍ２３→ルータＮ１５→通信装置Ｔ１２に自動的に変更されたとする。この場合、暗号装置Ｍ２１と暗号装置Ｍ２３との間で用いられる鍵（例えば鍵Ｂ）は、前述した鍵Ａとは異なっている。しかし、暗号装置Ｍ２１では、パケットの送信先（通信装置Ｔ１２）に変更がないので、通信装置Ｔ１１から通信装置Ｔ１２宛に送信されるデータの暗号用鍵を鍵Ａから鍵Ｂに変更すべきであることを従来のルーティングプロトコルからは認識することができない。そのため、当該パケットは暗号装置Ｍ２１で鍵Ａで暗号化されることになり、鍵Ｂを用いる暗号装置Ｍ２３ではこれを復号することができないので、結局、暗号通信を回復することができない。

【００１２】暗号通信には、送信先のアドレスを含むＩＰヘッダとパケットのデータ部分（すなわちペイロード）をまとめて暗号化し、新たな送信先（復号化装置）のアドレスを含むＩＰヘッダを付して通信を行うトンネルモードと、送信先アドレスは暗号化せず、パケットのデータ部分だけを暗号化するトランスポートモードとがあるが、いずれのモードでも、上記のように暗号装置Ｍ２２で障害が発生したときに、暗号装置Ｍ２１では鍵の変更の必要性を認識することができない。

【００１３】このような問題は、暗号通信中に経路障害が発生した場合のみならず、それまで最適経路であった箇所（ノード）に、新たにルータ、暗号装置、通信装置等が増設された場合や、ルータ等の一部が移動した場合においても共通に生じる。これは、従来のこの種の高可用通信におけるルータ等の配置が固定的であり、暗号通信に用いられる鍵も固定的であったことに起因する。

【００１４】そこで本発明は、高可用通信と暗号通信とが同時に実現できるネットワークにおいて、暗号化及び復号化を行う装置の配置構成に変更が生じた場合であっても、暗号用の鍵を動的に変更して暗号通信を安全に継続できるようにする技術を提供することを主たる課題とする。

【００１５】

【課題を解決するための手段】上記課題を解決ため、本発明は、改良された暗号通信方法、暗号通信システム、通信中継装置、及び通信中継装置をコンピュータにより実現する上で好適となる記録媒体を提供する。

【００１６】本発明の暗号通信方法は、高可用通信と暗号通信とを同時に実現することができるネットワークを介して行う方法であって、ネットワーク上で暗号通信可能な通信中継装置の配置に関する配置情報を含む所定の経路形成情報を複数の通信中継装置間で互いに交換しあうことによりネットワーク上における最適経路を形成し、この最適経路に存在する通信中継装置間で通信データの暗号通信を行うとともに、前記ネットワーク上における通信中継装置の構成が変更された場合に前記経路形成情報を更新して新たな最適経路を再形成し、再形成された最適経路に存する暗号通信可能な通信中継装置間で相互に取り決めた鍵を用いて前記暗号通信を継続することを特徴とする。各通信中継装置は、ある通信装置又はネットワークへ向かう暗号化された通信データの復号化ができる場合にその通信装置又はネットワークの識別情報を記録しておき、他の通信中継装置から経路形成情報を受け取ったときに暗号通信先が前記識別情報と同じ識別情報を保持していた場合に、前記他の通信中継装置との間で鍵の取り決めを行うようにする。

6

【００１７】本発明の暗号通信システムは、所定の経路形成情報を複数の通信中継装置間で互いに交換しあうことにより高可用通信と暗号通信とを同時に実現することができるネットワーク上における最適経路を形成し、この最適経路に存在する通信中継装置間で通信データの暗号通信を行う暗号通信システムである。各通信中継装置の経路形成情報は、前記ネットワーク上で暗号通信可能な通信中継装置の配置に関する配置情報を含むものであり、複数の通信中継装置の少なくとも一つは、暗号通信中の最適経路上の通信中継装置の配置構成が変更になったことを検知したときに当該変更後の配置情報を他の通信中継装置に通知するように構成され、少なくとも他の一つは、前記通知をもとに自己の経路形成情報を更新して新たな最適経路を再形成するとともに再形成された最適経路に存する暗号通信可能な通信中継装置間で相互に取り決めた鍵を用いて前記暗号通信を継続するように構成されていることを特徴とする。

【００１８】本発明の通信中継装置は、所定の経路形成情報をもとにネットワーク上における通信データの最適経路を形成するとともにこの最適経路に存在する他の通信中継装置との間で暗号通信を行う通信中継装置において、前記経路形成情報は、暗号通信可能な通信中継装置の配置に関する配置情報を含むものであり、暗号通信中に通信相手となる他の通信中継装置が通信不能になったときに自己の経路形成情報に含まれる前記配置情報の内容を更新する手段と、更新後の経路形成情報をもとに新たな最適経路を形成する手段と、新たに形成された最適経路上の暗号通信可能な他の通信中継装置を検出する手段とを備え、当該検出した通信中継装置との間で取り決めた鍵を用いて暗号通信を継続することを特徴とする装置である。

【００１９】経路形成情報は、より具体的には所定のルーティングプロトコルに基づいて他の通信中継装置との間で相互に受け渡しされる情報であって、暗号通信を行えるノードの配置に関する情報及びそのノードが暗号通信実施の対象とする通信経路の識別情報を含むものであり、この識別情報に基づいて前記鍵を取り決めるようにする。識別情報をもつノードとの間で取り決めた鍵を予

め保持している場合はその鍵を索出し、鍵を保持していない場合は当該ノードとの間で鍵生成を行うことで前記鍵を確保するようにする。

【００２０】通信中継装置における更新手段は、暗号通信中に通信不能となった通信中継装置がある場合はそれに関する配置情報を削除し、暗号通信中に増設された通信中継装置がある場合はそれに関する配置情報を追加し、暗号通信中に移動された通信中継装置がある場合はそれに関する配置情報を修正する。

【００２１】本発明が提供する記録媒体は、暗号通信可能な通信中継装置の配置に関する配置情報を含む所定の経路形成情報をもとに、高可用通信と暗号通信とを同時に実現することができるネットワーク上における最適経路を形成する機能と、通信相手装置との間で暗号通信を行う機能と、前記通信相手装置の構成が変更になった場合に自己の経路形成情報に含まれる前記配置情報の内容を更新し、更新後の経路形成情報をもとに新たな最適経路を形成するとともに、この新たな最適経路に存在する他の通信相手装置との間で取り決めた鍵を用いて暗号通信を継続する機能とをコンピュータ上に形成するためのプログラムコードが記録された、コンピュータ読みとり可能な記録媒体である。

【００２２】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を説明する。本発明では、高可用通信と暗号通信とが同時に実現できるネットワークにおいて、ルーティングプロトコルに従って経路形成情報の受け渡しを行う装置間で暗号通信を行っている場合に、暗号通信が可能な装置の配置に関する情報を上記経路形成情報に含め、経路形成情報と鍵の変更に関する情報とをリンクさせるようにする。例えば、リンクステート式のルーティングプロトコルであれば、どのリンクに暗号通信可能な装置が配置されていてどこのネットワーク間で暗号通信を行えるのか、ディスタンスベクトル式のルーティングプロトコルであれば、その距離ベクトル中にどのルータが存在するかを、経路形成情報の中に含める。そして、暗号化データを送信する際に、受信先の暗号装置に対応した鍵を用い、対応した鍵が無ければ新たに生成する、ということを容易に行えるようにする。なお、鍵の使用・生成は、従来から一般的に用いられていた手法を利用することができる。

【００２３】上述の暗号通信方法は、例えば図１に示すように構成される暗号通信システムによって実施することができる。この暗号通信システム１は、αネットワーク上に配された送信側の通信装置Ｔ１１、βネットワーク上に配された受信側の通信装置Ｔ１２、これらの通信装置間に介在する複数のルータ、すなわちＡルータＬ１１，Ｄルータ Ｌ１２，Ｂルータ Ｌ１３，Ｃルータ Ｌ１４その他のネットワーク構成部品を含み、高可用通信と暗号通信とを同時に実現できるように構成される。αネットワークとβネットワークとはインターネットのような広域通信網を介して接続されているものとする。

【００２４】各ルータＬ１１～Ｌ１４は、メモリ及びＣＰＵを有する一種のコンピュータであり、そのＣＰＵが所定の記録媒体に記録されたプログラムコードを読み込んで実行されることによって形成されるルーティングプロトコルの機能、暗号通信の機能、及び、これらの機能を連携させる機能を有する。このプログラムコードを記録した記録媒体は、ルータに実装されるときには、例えばＣＰＵが読みとり可能な半導体メモリ等の固定型記録媒体であるが、ＣＤ－ＲＯＭ等の可搬性記録媒体を通じて流通し、実装時に上記固定型記録媒体にインストールされるものであっても良い。ルーティングプロトコルの機能については、従来のルータのものと基本的には同じであるが、ルーティングプロトコルで他のルータと交換する経路形成情報に次の二つの情報を含め、暗号通信の機能を連携させるようにした点で従来のルータが備える機能と異なる。

（１）暗号通信を行えるノード（ルータ）の配置やインタフェースＩＤ

例：「暗号通信ができるＡノードにＡルータがある」

（２）そのノードが暗号通信実施の対象とする通信経路ＩＤ

例：「Ａルータにおける暗号通信の対象（通信経路ＩＤ）は、αネットワーク及びγネットワークの通信に対するものである」

これらの情報に対応するデータの形式は、適応するネットワークプロトコルやルーティングプロトコルに合わせたものになる。例えばＩＰネットワークのＯＳＰＦの場合は、後述するＬＳＡ（Link State Advertisement）にその情報を含めることになる。

【００２５】一方、暗号通信の機能に関して、各ルータは、以下のようにして暗号通信を行う。

（１）暗号通信実施対象の通信経路ＩＤに対応する通信に対して、通信データ、例えばパケットを暗号化し、暗号化データを生成する。

例：「Ａルータを通過するパケットのソースアドレスがγネットワークに属し、ディスティネーションアドレスがβネットワークに属するパケットは、ディスティネーションアドレスが通信経路ＩＤに適合するので、暗号通信の対象とする」

（２）暗号用の鍵は、通信経路に対応する通信経路ＩＤを持ったノードのものを予め保持している場合はそれを索出して使用する。鍵を保持していない場合は、そのノード（ルータ）との間で鍵生成を行うことで、鍵を確保する。

例：「Ａルータからβネットワーク宛の経路上に、Ｂルータという暗号通信が可能なルータが存在し、そのＢルータがβネットワークに対して暗号通信実施の対象としていることを、ルーティングプロトコルによりＡルータ

は知っている。そこで、暗号通信の対象となったパケットをＢルータに対応する鍵を使用して暗号化する」両者の機能をリンクさせる機能については後述する。

【００２６】なお、以上の機能は、全てのルータＬ１１～Ｌ１４が備えていることが望ましいが、通信装置Ｔ１１から送られたパケットを暗号化して中継するいずれか中心的に作用するルータのみが備えている場合であっても本発明の実施は可能である。

【００２７】次に、本実施形態の暗号通信システム１による通信形態を説明する。ここでは、図示のように、αネットワーク内の通信装置Ｔ１１とＡルータＬ１１間のネットワークアドレスが「163.135.10.0/24」、βネットワーク内の通信装置Ｔ１２とＢルータＬ１３又はＣルータＬ１４との間のインタフェースアドレスが「163.135.20.0/24」、ＡルータＬ１１のインタフェースアドレスが「163.135.100.10」、ＢルータＬ１３のインタフェースアドレスが「163.135.200.20」、ＣルータＬ１４のネットワークアドレスが「163.135.300.30」であるものとし、リンクステート式ルーティングプロトコルの代表である上記ＯＳＰＦの改良を行って暗号通信を行う場合の例を挙げる。ＯＳＰＦについては、国際機関IETFで発行している仕様RFC2328、RFC1131、STD0054に詳細に記載されている。

【００２８】ＯＳＰＦで使用される経路形成情報、すなわちリンク状態広告パケット（ＬＳＡ：Link State Advertisement）のうち、各ルータＬ１１～Ｌ１４が送信するルータリンクＬＳＡのフォーマット例を図２に示す。このルータリンクＬＳＡは、隣設ルータ間で受け渡される各種リンク情報であり、リンク状態ヘッダとＬＳＡ部とから構成される。ＬＳＡ部には、ルータタイプ、リンクＩＤ、リンクデータ等が記述されており、これに記述される情報によって各ルータが他のルータの配置に関する情報を認識でき、経路計算、又は再計算に利用することができるようになる。図３は、ルータタイプの内容と、それに対するリンクＩＤ、リンクデータの例とを示したものである。タイプ１～４は、既存のルータが具備する情報であり、タイプ５が、本実施形態で追加した部分、つまり、暗号通信に関連する情報である。このタイプ５の記述によって、どのルータがどこで暗号通信を行っているかをわかるようにする。タイプ５において、リンクデータがＮｕｌｌの場合は、まだ決定されていないどこかと暗号通信ができることを示す。

【００２９】ＬＳＡは、各ルータＬ１１～Ｌ１４で持てるリンク情報を複数発信することができる。従って、一つのルータが複数のルータとの間で暗号通信を行っていれば、暗号通信用ＬＳＡも複数指定できる。例えば、タイプ５のＬＳＡでリンクＩＤが「163.135.100.10」、リンクデータが「163.135.20.0/24」であれば、このＬＳＡを送信した「163.135.100.10」をアドレスとして持つルータは、「163.135.20.0/24」というアドレスを持つ相手先と暗号通信ができる状態であることを示す。さらに、リンクＩＤまで同じで、リンクデータ「163.135.30.0/24」のＬＳＡがあれば、ルータ「163.135.100.10」は、「163.135.30.0/24」の相手先とも暗号通信ができる状態であることを示す。

【００３０】このような改良ＯＳＰＦを使用し、パケットを暗号化して送信する場合、各ルータＬ１１～Ｌ１４は、暗号通信先の情報をＬＳＡで宣言することになる。この宣言には、暗号通信元の情報も含まれる。各ルータＬ１１～Ｌ１４は、また、あるネットワークへ向かうパケットの復号化ができる場合、ルータ自身のデータベースにそのネットワークの情報を「暗号通信受け持ちネットワーク（又はホスト）」として記録する。この情報は、各ルータが、他のルータの暗号通信ＬＳＡを受け取ったときにその暗号通信先と同じ「暗号通信受け持ちネットワーク」を持っていた場合に、そのＬＳＡ送信元ルータとの間で鍵生成を行うために必要な情報となる。

【００３１】ルータ同士は、それぞれＨｅｌｌｏパケット（隣接ルータに対するキープアライブ信号のようなもの）の受け渡しを行っており、この受け渡しが可能なルータ間では、それぞれ自己のＬＳＡがリンクーバイーリンクで相手側に伝わるようになっている。例えば、ＢルータＬ１３及びＣルータＬ１４が暗号化及び復号化が可能なルータである場合は、その旨及びそれが正常に動作していることが、ＤルータＬ１２を通じてＡルータＬ１１に伝わる。ＡルータＬ１１は、ＢルータＬ１３のＬＳＡにより、そのルータＬ１３が自己の「暗号通信受け持ちネットワーク」と暗号通信を行う用意があることを知り、ＢルータＬ１３との間で暗号用の鍵を生成するプロセスを実施する。このプロセスは、一般に用いられている鍵生成のプロセスであって構わない。ＡルータＬ１１は、また、ＣルータＬ１４との間でも鍵を生成するプロセスを実施する。

【００３２】図４（ａ）は、通常経路で収束したときのＡルータＬ１１のリンクテーブル（ルーティングテーブルの元情報）の内容を示した図である。図示の例では、ＡルータＬ１１は、αネットワーク及びＤルータＬ１２とリンクしており、暗号通信受け持ちネットワークはαとγである。ＢルータＬ１３，ＣルータＬ１４は、βネットワークとＤルータＬ１２とリンクしており、「暗号通信受け持ちネットワーク」は共にβである。Ｄルータは、ＡルータＬ１１，ＢルータＬ１３，ＣルータＬ１４とリンクしており、「暗号通信受け持ちネットワーク」の指定がない又は未だ決定されていないどこかである。なお、「暗号通信受け持ちネットワーク」は、必ずしも隣接している必要はない。

【００３３】このリンクテーブルから、ＡルータＬ１１は、ネットワークαからネットワークβへの最適経路を、αネットワーク（通信装置Ｔ１１）→ＡルータＬ１１→ＤルータＬ１２→ＢルータＬ１３→βネットワーク

（通信装置Ｔ１２）のように形成する。

【００３４】一方、ＡルータＬ１１は、図４（ａ）のリンクテーブルと連携して暗号化フィルタを図５（ａ）のように設定する。すなわち、ＡルータＬ１１の「暗号通信受け持ちネットワーク」はαネットワークであり、経路上にβを「暗号通信受け持ちネットワーク」とするルータはＢルータＬ１３である。そこで、ＡルータＬ１１は、ＢルータＬ１３との間で鍵ａの生成を行う（鍵ａを既に保持してある場合は、それを索出する）。このリンクテーブルの意味は、「発信元アドレス（ネットワーク）がαで、送信先アドレス（ネットワーク）がβのパケット（α→β）を、鍵ａで暗号化してＢルータＬ１３へ送信（set peer(B)）せよ」である。これにより鍵ａを用いた暗号通信が可能になる。

【００３５】ここで、ＢルータＬ１３に障害が発生した場合を考える。この場合は、ＢルータＬ１３が発するＬＳＡがＤルータＬ１２及びＡルータＬ１１に届かないため、ＡルータＬ１１は、ルーティングプロトコルの機能を用いてＢルータＬ１３が使えないものとして経路を回復させる。図４（ｂ）は、回復経路で収束したときのＡルータＬ１１のリンクテーブル（ルーティングテーブルの元）の更新後の内容を示した図である。図示のように、ＢルータＬ１３のリンク情報が無くなっている。このリンクテーブルから、最適経路は、αネットワーク（通信装置Ｔ１１）→ＡルータＬ１１→ＤルータＬ１２→ＣルータＬ１４→βネットワーク（通信装置Ｔ１２）のように変更されるが、本実施形態では更に、経路変更と連携してＡルータＬ１１が使用する鍵ａを鍵ｃに動的に変更させる。

【００３６】すなわち、ＡルータＬ１１は、図４（ｂ）のリンクテーブルが更新されると、これに連携して暗号化フィルタの内容を図５（ｂ）のように更新する。すなわち、経路上にβを「暗号通信受け持ちネットワーク」とするルータはＣルータＬ１４であることがわかるので、ＡルータＬ１１は、ＣルータＬ１４との間で鍵ｃの生成を行う（鍵ｃを既に保持してある場合は、それを索出する）。このリンクテーブルの意味は、「発信元アドレス（ネットワーク）がαで、送信先アドレス（ネットワーク）がβのパケット（α→β）を、鍵ｃで暗号化してＣルータＬ１４へ送信（set peer(B)）せよ」である。

【００３７】このように、ＢルータＬ１３に障害が発生し、経路変更がなされても、更新後のルーティングプロトコルによるリンクテーブルから図５（ｂ）のような暗号化フィルタの設定が得られ、経路変更に伴う鍵の変更がなされるので、暗号通信を継続できるようになる。

【００３８】なお、本実施形態では、暗号通信可能なルータの配置構成に変更が生じ、これによって使用する鍵が変更される場合の例として、ルータの故障等による経路障害が生じたことを想定したが、本発明は、このような例のみではなく、例えばネットワーク上にルータを増設し、あるいはあるネットワークから他のネットワークにルータを移動させた結果、使用する鍵が変更される場合にも同様に適用が可能である。すなわち、手動による暗号通信の設定を行うことなく、ルーティングプロトコルの機能を用いて相互に経路形成情報を受け渡し、その配置情報を各ルータで更新し、最適経路を自動的に形成することで、暗号通信を継続することが可能である。また、ルータの経路形成情報に、暗号通信を行う対象のネットワークないしホストを指定するだけで、当該ルータが自動的に暗号通信を行う相手先装置を見つけ出すことも可能となる。これらの機能は、あるネットワーク上に接続されるルータの数が絶えず増減するという現実の通信形態に即した機能であり、これによってモバイル型通信の普及にも容易に対応が可能になるものである。

【００３９】本実施形態では、通信中継装置としてルータを例に挙げて説明したが、本発明の仕組みは、暗号通信の相手先が変化する場合のある装置全般に適用することが可能である。また、本実施形態のように経路形成情報を他の装置と相互に受け渡す機能と暗号用の鍵を動的に変更させる機能とを一つの装置（例えばルータ）内に設けることは好ましい形態であるが、常にこのような形態にしなければならないというものではない。例えばルータに接続された通信装置が、ルータからの通知に基づいて暗号用の鍵を動的に変更する機能をもつように構成することは、本発明の暗号通信方法を実施する上で支障とはならない。

【００４０】本実施形態では、ＩＰネットワークを通信媒体とした例について説明したが、本発明は、高可用通信と暗号通信とを同時に実現することができるネットワークであれば、その規模にかかわらず適用が可能なので、アンセキュアなネットワークであるイントラネットやエクストラネットでの利用も可能である。

【００４１】本発明の適用には、ルーティングプロトコルのような経路形成情報の相互受け渡し機能が前提となるため、他の独自のルーティングプロトコルを使っていたり、ルーティングプロトコルの相互接続ができないＩＳＰ（Intarnet Service Provider）を利用する場合は、そのＩＳＰを利用しない閉域網内で利用することになるが、そのＩＳＰを利用した場合であっても、経路形成情報を公知のトンネリング技術でＩＳＰのサービスによらない方法で中継することにより、閉域網を越えたネットワークでの利用も可能である。

【００４２】本発明は、暗号通信先が物理的もしくは論理的に頻繁に変更になる場合に特に有効であり、モバイルネットワークといった網構成変更にも柔軟に対応が可能である。

【００４３】本発明は、また、コンシューマ用暗号通信市場（個人を対象としたネットワークサービスの利用の一形態）への適用も可能である。現在、個人を対象とし

13

た暗号通信技術の主流はＳＳＬ（Secure Socket Layer）である。これは、通信の上位層で暗号化するもので、個人が操作する端末（通信装置）自らが通信データを暗号化して送信することによりエンド・ツー・エンドの暗号通信を行うことを目的とする。本発明をこの個人が操作する端末（モバイル型端末を含む）がアクセスするネットワークに適用させることは、上記ネットワークサービスを促進する上で有効な手段となり得る。

【００４４】

【発明の効果】以上の説明から明らかなように、本発明によれば、暗号通信中に経路変更が行われた結果、復号化する装置、つまり鍵に変更が生じた場合であっても、暗号通信を安全且つ確実に継続できるようになるという、特有の効果がある。

【図面の簡単な説明】

【図１】本発明を適用した暗号通信システムの構成図。

【図２】ルータリンクＬＳＡのフォーマット例を示した図。

【図３】ルータリンクＬＳＡのタイプ種類を示した図。＊

14

＊【図４】（ａ）は、ルーティングプロトコルを用いた場合の最適経路を形成する場合に使用されるリンクテーブルの内容説明図、（ｂ）は障害発生時に更新されるリンクテーブルの内容説明図。

【図５】（ａ）は、正常動作時における暗号化フィルタの設定内容を示した図、（ｂ）は障害発生時に更新される暗号化フィルタの設定内容を示した図。

【図６】従来における、ルーティングプロトコルを用いた場合の最適経路復旧の説明に用いるためのネットワーク構成図。

【図７】従来における、ルーティングプロトコル及び暗号通信を用いた場合の最適経路復旧の説明に用いるためのネットワーク構成図である。

【符号の説明】

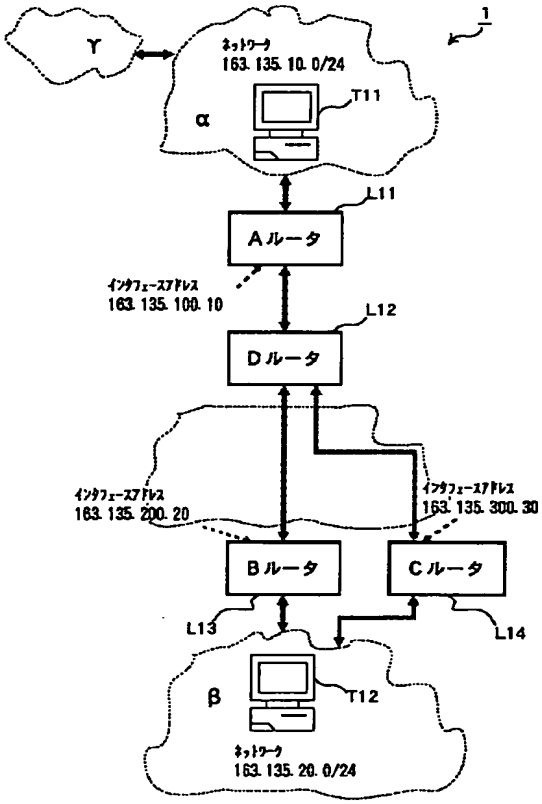
１　　暗号通信システム

Ｔ１１，Ｔ１２　通信装置

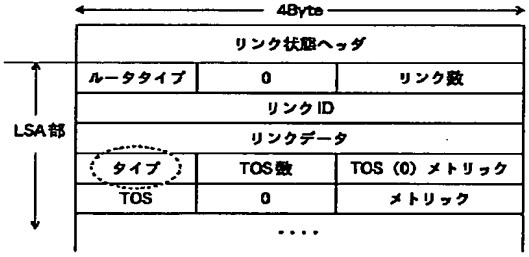
Ｌ１１～Ｌ１４，Ｎ１１～Ｎ１５　ルータ

Ｍ２１～Ｍ２３　暗号装置

【図１】



【図２】



【図３】

タイプ	内容	リンクID	リンクデータ
1	他のルータへのポイント・ツー・ポイントコネクション	隣接ルータのルータID	インタフェース番号（またはIPアドレス）
2	通過ネットワークへのコネクション	代表ルータへのアドレス	ルータのそのネットワーク上のIPアドレス
3	スタブ・ネットワークへのコネクション	サブネットワークに対する、アドレスプレフィクス	プレフィクス長
4	仮想リンク	隣接ルータのルータID	ルータのそのネットワーク上のIPアドレス
5（追加する部分）	暗号通信	暗号通信ができる自ノードのIPアドレスかルータID、またはインタフェース番号、またはインタフェースのIPアドレス	暗号通信ができる相手先のネットワークアドレスまたはホストアドレス

【図４】

(a)

ルータ	A	B	C	D
持っているリンク（コスト）	α (1) D (1)	β (1) D (1)	β (1) D (2)	A (1) B (1) C (2)
暗号通信受け待ち ネットワーク	α γ	β	β	N/A

(b)

ルータ	A	C	D
持っているリンク（コスト）	α (1) D (1)	β (1) D (2)	A (1) B (1) C (2)
暗号通信受け待ち ネットワーク	α γ	β	N/A

【図５】

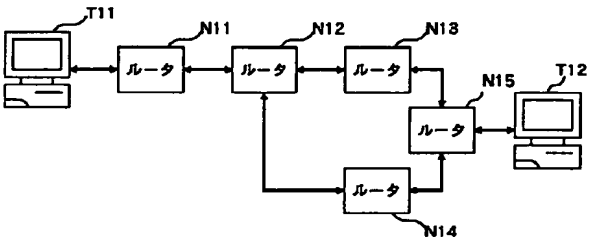
(a)

match	α→β
set peer	(B)
key	a

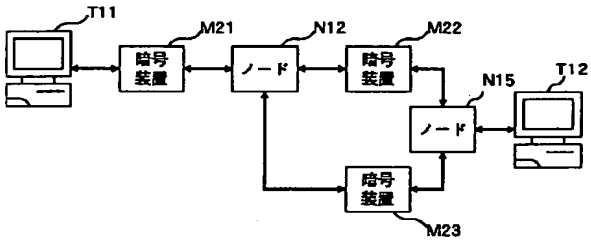
(b)

match	α→β
set peer	(C)
key	c

【図６】



【図７】



フロントページの続き

(51)Int.Cl.⁷ 識別記号 F I テーマコード（参考）
H04L 29/14

(72)発明者 馬場 達也
東京都江東区豊洲三丁目３番３号 株式会社エヌ・ティ・ティ・データ内

Fターム(参考) 5J104 AA01 AA34 BA02 NA02 NA37 PA07
5K030 GA12 GA15 HD03 KA05 LB05
5K033 AA06 AA08 CB08 DA05 DB18 EC03
5K035 CC09 DD01 LL17
9A001 BB02 BB04 CC06 CC07 DD10 EE03 HH09 JJ18 LL07 LL09